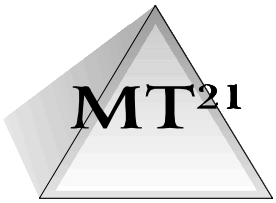

ENTERPRISE STANDARDS AND POLICIES

During the past few years, several white papers and working draft documents have been published to identify directions, policies, procedures, standards, and recommendations for the acquisition and management of enterprise information technology resources. The following is a summary of these works.

ENTERPRISE INFORMATION SYSTEM

In 1994, a draft document was developed detailing the implementation of the enterprise information system (Novell 4.x implementation). The "Enterprise Information System for State of Montana" document has been adopted by ITMG.

ITMG DATABASE DIRECTIONS

In 1993, ITMG adopted the "Database Directions" document, which defines standards

and guidelines for the selection of database software. Since then, the state has established Oracle as the enterprise database standard. The following summarizes key standards and recommendations from the Database Directions document:

- Open standards.
- Relational architecture.
- SQL-89 conformance.
- Integrity services controlled by the RDBMS.
- Record locking, application rollback, application resource release, and deadlock detection.
- Full distributed transaction support for distributed systems.
- Functionally rich set of utilities for support and development.
- Support for a variety of programming languages, both 3GL and 4GL.
- Open system approach to OLTP.
- Support of numerous vendor software offerings for client/server and GUI applications with Remote Data Management (RDM).
- Data dictionary or catalog structures maintained through SQL commands.
- Standard security via user identification and password validation with cooperation with external security systems in place on that platform.
- Data integrity through recovery with rollback, journaling, and recovery facilities.
- Backup facilities allowing for continuous operations.
- Robust end-user capabilities.
- ANSI and ISO standards conformance.
- Access to non-relational data.
- Portability or communication with multiple platforms.
- Support of state network protocols.
- Use of existing development skill set.
- Languages and tools that work on multiple hardware/operating system environments.

IMAGING

In 1996, ITMG and ITAC adopted the "Electronic Imaging Standards" document. Management and technical issues relating to the following subjects are addressed within that document.

- Document Processing and Workflow
- Storage
  - Recording Permanence
  - Storage Environment
- Legal Considerations
  - Evidence and Authenticity Requirements
- Retention Schedules
- Public Access and Privacy
  - Segregating Exempt and Non-exempt Information
  - Access Through Time
  - Ability to Make Copies
- Technical Documentation
  - System Documentation
- Operational Documentation
- Security
- Legal Expungement
- Integration with Existing and Other Information Systems
- Scanner
- Quality Control
- Conversion
  - In-house Conversion
  - Service Bureau/Imaging Contracted Services Conversion
- Indexing
  - Index Location
  - Indexing Parameters
  - Index Data Entry
- Security
  - Media Selection
  - Backup
  - Access Restrictions
- System Migration

Vendor Stability
System Obsolescence
Media Longevity
Migration Strategies

- ▲ Disaster Recovery
- ▲ Planning

MID-TIER COMPUTING

The following standards and recommendations are contained in the "Report of Mid-Tier Computing Standards and Recommendations" document adopted by ITMG and ITAC in 1995:

1. Operating System (OS)

A. General OS

Standard

- ▲ The State supports dual OS standards for mid-tier systems. The operating systems are UNIX and Windows NT.

B. UNIX OS

Standards — UNIX OS MUST:

- ▲ be POSIX compliant.
- ▲ be SPEC1170 compliant.
- ▲ be XPG3 branded. The OSMUST continue to meet UNIX branding standards as they evolve.
- ▲ support application independence by being able to run applications that are not married to either the OS or the hardware platform.
- ▲ adhere to standards-based APIs that facilitate the porting of applications from one system to another.

Recommendations — UNIX OS:

- ▲ SHOULD NOT contain any proprietary APIs that, if used, would compromise the goal of application portability (i.e. general business applications, excluding Oracle).
- ▲ MAY contain proprietary APIs for use by general system utilities, such as system management and backup/restore.
- ▲ SHOULD support the Open Systems Foundation (OSF) Distributed Computing Environment (DCE) standards.
- ▲ SHOULD support symmetric multiprocessing (SMP).

C. Portable OS

Standards — The portable OS MUST:

- ▲ provide application portability/independence from specific hardware platforms.

- ▲ be capable of running on several types of processors (e.g. Intel, Alpha RISC, and PowerPC).

Recommendations — The portable OS SHOULD:

- ▲ support DCE standards.
- ▲ support SMP.

2. Hardware

Standards — Mid-tier hardware MUST:

- ▲ have a native operating system that complies with either of the two OS standards described above.
- ▲ provide a linear upgrade path for uniprocessor configurations.
- ▲ provide performance and capacity scalability for I/O subsystems.
- ▲ provide memory scalability.

Recommendations — Mid-tier hardware SHOULD:

- ▲ support industry standard I/O subsystems.
- ▲ provide high availability.
- ▲ offer clustering capabilities.

3. Platform

A. General

Standards — Mid-tier platform:

- ▲ MUST support both Token Ring and Ethernet.
- ▲ MUST support TCP/IP in a router based environment.
- ▲ MUST be able to run Oracle's database application.
- ▲ MUST interface with SNADS, our existing enterprise e-mail standard (DISOSS and ZIP!Mail/ZIP!Office).
- ▲ SHOULD be able to run mail products that are based upon open standards such as X.400, X.500, and SMTP.
- ▲ MUST support TCP/IP connectivity between desktop clients (e.g. DOS, Windows 3.1, X/Windows (Motif & OpenView), OS/2, Macintosh, etc.), other mid-tier servers, and mainframes (e.g. MVS, VSE, VM, VMS, etc.)

Recommendations — Mid-tier platform SHOULD:

- ▲ provide SQL-based access to the State's relational and non-relational data (e.g. IDMS, VSAM, R:Base, dBase) on interconnected, multi-vendor platforms.
- ▲ provide transparent user access to data regardless of location or file structure.
- ▲ be NDS aware.
- ▲ support a generic IPX connectivity (OSI Layer 3 & NetWare Core Protocol) to desktop clients (e.g. DOS, Windows 3.1, OS/2, Macintosh, etc.)
- ▲ be SNMP monitorable.
- ▲ support the following set of sockets and services:
  - — generic (OSI Layer 3 & 4) TCP/IP based clients
  - — TCP/IP communications between peer mid-tier and mainframe platforms
  - — TELNET client & server connectivity

- FTP server & client services
- SNMP monitoring
- support for SMTP

▲ support generic DECnet (OSI Layer 3) based clients.
▲ support a full feature implementation of SNA, including communication with an IBM host via LU 6.2/APPC.
▲ support telephony control or access.
▲ support or give access to a wide variety of file types, including DOS, HPFS (OS/2,NT), NFS, and DEC.
▲ support the following domain schemes: Novell NetWare Directory Services, TCP/IPs Domain Name Services, and the X.500 standard.
▲ support systems management software that supports operations management, performance management, storage management, security management, and change management.

B. Platform Security

Standard

▲ Mid-tier platform security MUST support, at a minimum, a C2 level of security.

Recommendation

▲ Platform security for systems requiring data encryption/decryption across the network SHOULD use the DCE implementation of network encryption.

4. Applications

A. General

Recommendations

▲ Mid-tier application software SHOULD support the OSF DCE standards.
▲ Mid-tier applications SHOULD not be written using proprietary operating system services which would limit their cross-platform portability.
▲ Mid-tier application developers SHOULD understand that the use of platform specific APIs, like DDE and OLE, could reduce the applications cross-platform portability.

B. Disaster Recovery

Recommendations

▲ Disaster recovery standards for each mid-tier application SHOULD require and/or define:
  - Backup methods (Full; incremental, preferably with a periodic verification backup; or selective? Automatic or manual?). Procedures for off-site storage of backup data; supporting software (for the application itself plus backup tools, tracking, and recovery software); supporting manuals; and any other documentation needed to facilitate recovery (hardware configuration diagrams, vendor/employee notification lists, critical forms, etc.).

- A strategy for restoring the application (documented in written form as a disaster recovery plan).
- A testing program for validating, improving, and maintaining the recovery plan.
- A training program for ensuring that employees can implement the plan, there is sufficient cross-training of recovery staff, and potential threats to the application are recognized and eliminated, or reduced, as appropriate.

▲ Disaster recovery standards SHOULD be drafted so that:

- Ownership and responsibility for applications and the mid-tier platforms upon which they reside, are clear-cut.
- Controls for managing the development and maintenance of software, for ensuring data integrity, and for adequately protecting physical and logical access are well established.
- Standardization is promoted in terms of hardware, software, backup systems, etc. Any exceptions to the standards SHOULD be identified, and planned for, within each application's disaster recovery plan.
- Recovery priorities are established for applications and data. During a recovery, the set of systems available for recovery is limited, so only a relatively small percentage of total data and applications can be restored. Therefore, applications SHOULD be ranked in terms of their:
  - Criticality: What negative impacts would result (financial, legal, goodwill, others) from the loss of a particular application? AND
  - Interdependencies: Do critical applications depend upon other applications or shared data?

  To help ensure that critical data and applications can be restored quickly, mid-tier applications standards could provide recommendations (or mandates) that support the ranking of applications for disaster planning purposes. For example, standards could specify how directories SHOULD be established to segregate categories of critical, essential, and nonessential data.

C. OLTP Software

Recommendations — OLTP Software SHOULD:

▲ support ISO's Open Systems Interconnection (OSI) and X/Open's Distributed Transaction Processing (DTP) standards.

▲ offer support for the CICS API.

5. Vendor

A. Vendor Viability

Recommendation — The vendor MUST:

▲ demonstrate long-term viability including, but not limited to, meeting a minimum number of years in business standard; posting a performance bond of an amount commensurate with the state's potential loss; and furnishing references of installations

that are similar to the state's profile.

B. Vendor Service Support

Recommendations:

- ▲ Service providers will be evaluated by service offerings, level of service, business practices, and delivery capabilities.
- ▲ Service providers SHOULD offer several options, based on response times, spare parts inventory, and self maintenance.
- ▲ Service provider MUST offer an option to train users in self-maintenance.
- ▲ Service provider MUST be willing to assume some responsibility for third-party product support.
- ▲ Service provider MUST provide coverage for Helena and outlying locations.
- ▲ It would be very desirable for the service provider to locate a service technician in Helena.
- ▲ Service provider MUST maintain an inventory of critical component spare parts at its main Montana service location.
- ▲ Service provider MUST be held to maximum response and repair time frames in Helena and outlying locations.

C. Disaster Recovery Assistance

Recommendation — Mid-tier vendor SHOULD:

- ▲ provide disaster recovery assistance.

D. ISV Support

Recommendation — Mid-tier vendor MUST:

- ▲ have widespread and proven ISV support in areas including vertical applications, productivity applications, and systems/network management tools.

PERSONAL COMPUTER DIRECTIONS

In 1991, the "Personnel Computer Directions" document was drafted to record the basis of several decisions regarding personal computer hardware and software. The following summarizes these decisions:

- ▲ IBM PC/Intel is the standard personal computer platform.
- ▲ New microcomputer acquisitions must be made using the state microcomputer term contracts.

DATA SHARING RESOLUTION

The following resolution was adopted by the Data Processing Advisory Council at their November 5, 1992 meeting:

DATA PROCESSING MANAGERS' GROUP RESOLUTION:
DATA SHARING
AUGUST 12, 1992

WHEREAS, a tremendous amount of electronic data is being maintained by state agencies, and;

WHEREAS, the duplication of electronic data will continue to increase if systems are developed without consideration for the sharing of data with other agencies, and;

WHEREAS, the cost of capturing, processing, and analyzing electronic data can be minimized for the state as a whole if more data sharing takes place between agencies;

NOW, THEREFORE BE IT RESOLVED by the Data Processing Managers' Group that it is a goal of state agencies to share data with other agencies whenever possible, if not prohibited by legal confidentiality requirements. Therefore, during major system development and enhancement projects, all state agencies should consider other agencies' automated systems in their design plans as an alternative to creating redundant data and/or systems within their own agency;

AND, BE IT FURTHER RESOLVED by the Data Processing Managers' Group that agencies should develop systems using software that meets compatibility criteria developed, with agency involvement, by ISD. The criteria should be developed with the purpose of ensuring that agencies acquire and use hardware and software that enable data to be shared among agencies.

SUMMITNET ACCEPTABLE USE POLICY

SummitNet Defined

SummitNet is the state's telecommunications nucleus network, or backbone, connecting agency, University, K-12, library, and local government networks. SummitNet provides connectivity to the Internet, the world's largest network of individuals, governments, organizations, universities, schools, and companies.

SummitNet's telecommunications users are elected officials, state and local government employees, educators, students, researchers, authorized contractors, and non-profit organizations. Through SummitNet, these authorized users can access a wide range of national and international information. This access empowers them in becoming active producers of information rather than passive consumers.

SummitNet Acceptable Use

SummitNet is to be used for: the conduct of state and local government business and delivery of government services; the support of instruction, learning, training, educational administration, research, and grant procurement; the increased participation

of citizen oversight of government affairs; and the promotion of economic development.

SummitNet users may be subject to restrictive or limited use of the network, including access to the Internet, as determined by a supervising authority or administrator.

Internet Acceptable Use

Internet is to be used for the transmitting and sharing of information among governmental, research, and educational organizations. SummitNet users may access the Internet to: support open research and education in and between national and international research and instructional institutions; communicate and exchange professional information; encourage debate of issues in a specific field of expertise; apply for or administer grants or contracts; announce requests for proposals and bids; announce new services for use in research or instruction; and conduct other appropriate state business.

SummitNet and the Internet are not to be used for "for-profit" activities or for extensive use for private, recreational, or personal business.

Public Access to SummitNet and the Internet

Private citizens may access SummitNet through the Internet. This Internet access can be obtained through a subscription with a private Internet service provider.

Remote Dial-In Access to SummitNet and Internet

Users who access SummitNet through remote dial-in are to honor and observe this SummitNet Acceptable Use Policy as well as other acceptable use policies defined by networks which they access through SummitNet. Acceptable Use Policy violations by remote dial-in users should be reported to personnel responsible for local network policy enforcement, or to Security Officers with the Department of Administration, Information Services Division.

User Responsibilities Related to SummitNet and Internet Acceptable Use

SummitNet and Internet users are responsible for:

- honoring acceptable use policies of networks accessed through SummitNet or the Internet.
- honoring existing federal, state, and local telecommunications and networking laws, regulations, and policies.
- using SummitNet and the Internet for state and local government business and educational purposes and not for illegal and for-profit, private, or personal business purposes and activities.
- reporting to the appropriate authority the violation of any network Acceptable Use Policy.
- honoring copyright laws regarding protected commercial software or intellectual property.

- demonstrating respect for an individual's right to privacy and to freedom from intimidation, harassment, and unwarranted annoyance.

- minimizing unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource; such as, refraining from monopolizing systems; overloading networks with excessive data; or wasting computer time, connect time, disk space, or other resources.

Policy Enforcement

Several tiers or levels of networks and network management are involved with acceptable use policy enforcement. These tiers of networks are:

(1) SummitNet Tier (State's telecommunications *backbone network* governed by the SummitNet Executive Council. Network managed by the Department of Administration's Information Services Division personnel).

(2) Logical Tier (Networks *directly connected* to SummitNet. Managed by University, Agency, Enterprise Entity personnel).

(3) Satellite Tier (Networks connected to Logical Networks. Satellite networks managed by local personnel or by Logical Tier Network personnel).

Administrative or network management personnel at each tier will enforce the SummitNet Acceptable Policy and their local acceptable use policy.

Policy Violation

Users of networks are responsible for honoring the SummitNet Acceptable Use Policy and acceptable use policies of networks they access. *Users are also responsible for reporting acceptable use infractions or violations* to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies *where the violation originated*.

Personnel reviewing the reported acceptable use policy violation will determine the validity and severity of the violation and will follow local procedures for dealing with and correcting infractions and violations. These steps will be in-line with existing state and federal laws, polices, and procedures as related to personnel and network management. Violation enforcement may result in an appeal process pursued by the offender, with the highest level of appeal being the SummitNet Executive Council (SEC).

In some cases, the severity of the violation may mandate that it be reported to a higher network tier manager or security officer. The highest tier for reporting is the SummitNet Tier managed by Information Services Division. Once the reported violation reaches this tier, it may involve the Attorney General and Legislative Auditor's Office.

Network monitors at any tier (personnel who monitor the network, network services, and network information for security and/or network management reasons) may also report acceptable use infractions or violations. These network monitors will follow the same tier approach, as defined in the foregoing paragraph, when reporting violations.

References

2-15-114, MCA; 2-17-302, MCA (ARM 2.13.101-2.13.107); 2-17-503, MCA; 45-6-311, MCA.

Disclaimer

The SummitNet Executive Council reserves the right to modify this policy at any time. Adopted by the SummitNet Executive Council on November 1, 1995.